National Cybersecurity Center of Excellence

Michael Powell, Principal Investigator

Manufacturing Sector Community of Interest Call

Manufacturing_nccoe@nist.gov

February 25, 2021

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SP 1800-10: Detecting and Protecting Against Data Integrity Attacks in Industrial Control Systems (ICS) Environments

Project Focus:

- Help manufacturing organizations detect and protect against data integrity attacks

Project Scope:

- Provide an approach to help manufacturers prevent, mitigate, and detect threats from cyberattacks or insider threats within an ICS environment
- Demonstrate how commercially available technologies deployed in this build can provide cybersecurity capabilities that manufacturing organizations can use to secure their operational technology (OT) systems

Cybersecurity Capabilities

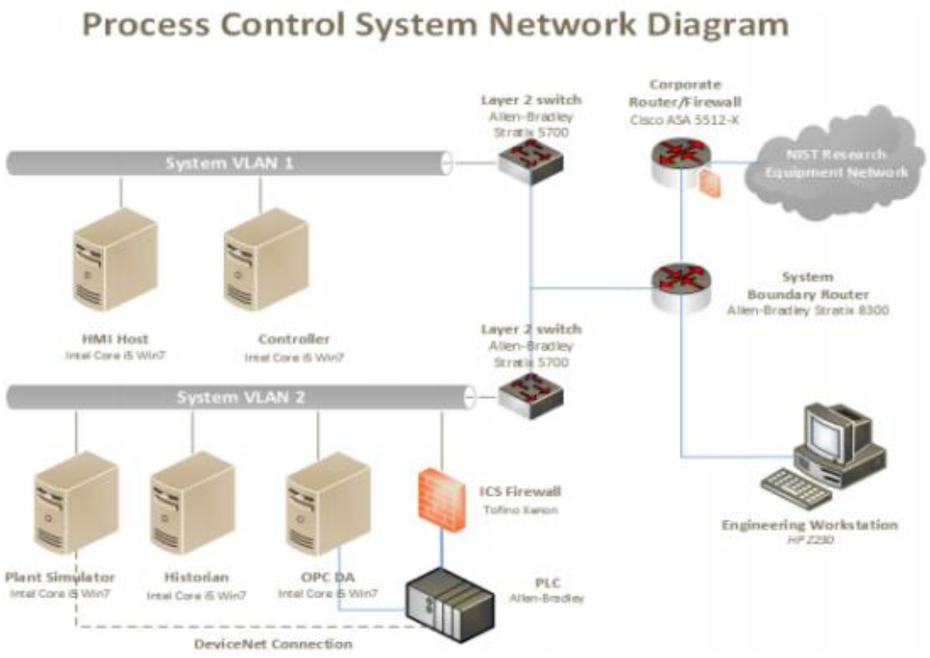
SP 1800-10 Detecting and Protecting Against Data Integrity Attacks in ICS Environments

- behavioral anomaly detection
- security incident and event monitoring
- ICS application whitelisting
- malware detection and mitigation
- change control management
- user authentication and authorization
- access control least privilege
- file integrity checking mechanisms

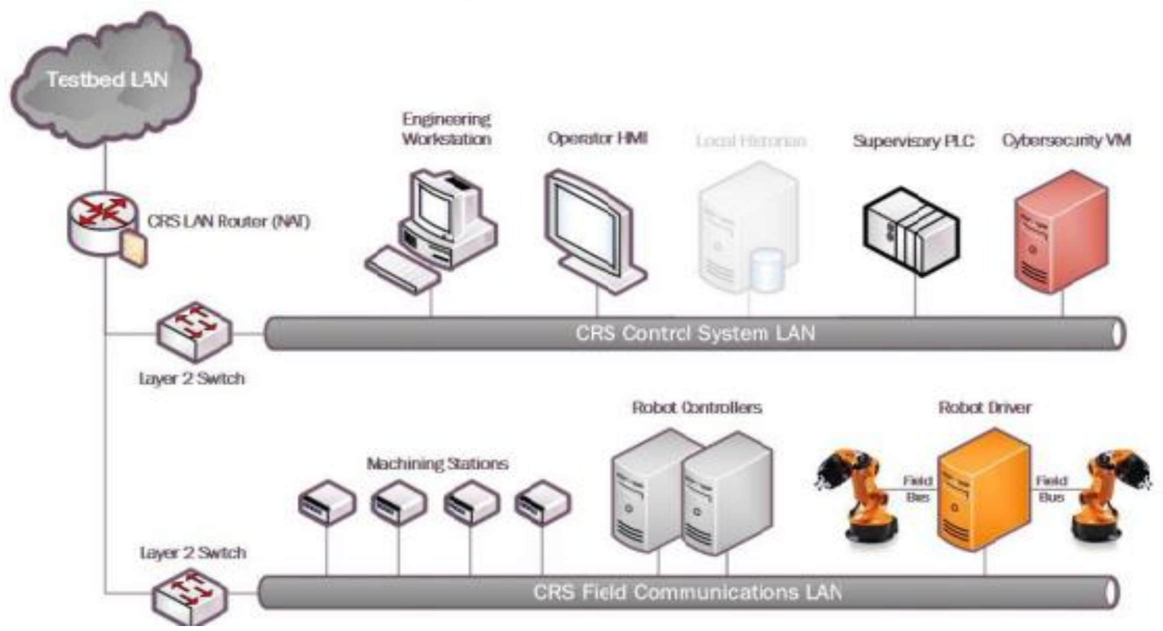
Multiple Capabilities in Two Manufacturing Demo Environments

Detecting and Protecting Against Data Integrity Attacks in ICS Environments

Process Control System Architecture



Robotics-Based Manufacturing Workcell Architecture



The Manufacturing Project Team

- The NIST Engineering Lab
- NCCoE Staff
- Collaborators

Microsoft | CYBERX

DISPEL

DRAGOS

FORESCOUT

GreenTec™
www.GreenTec-USA.com

OSIsoft.

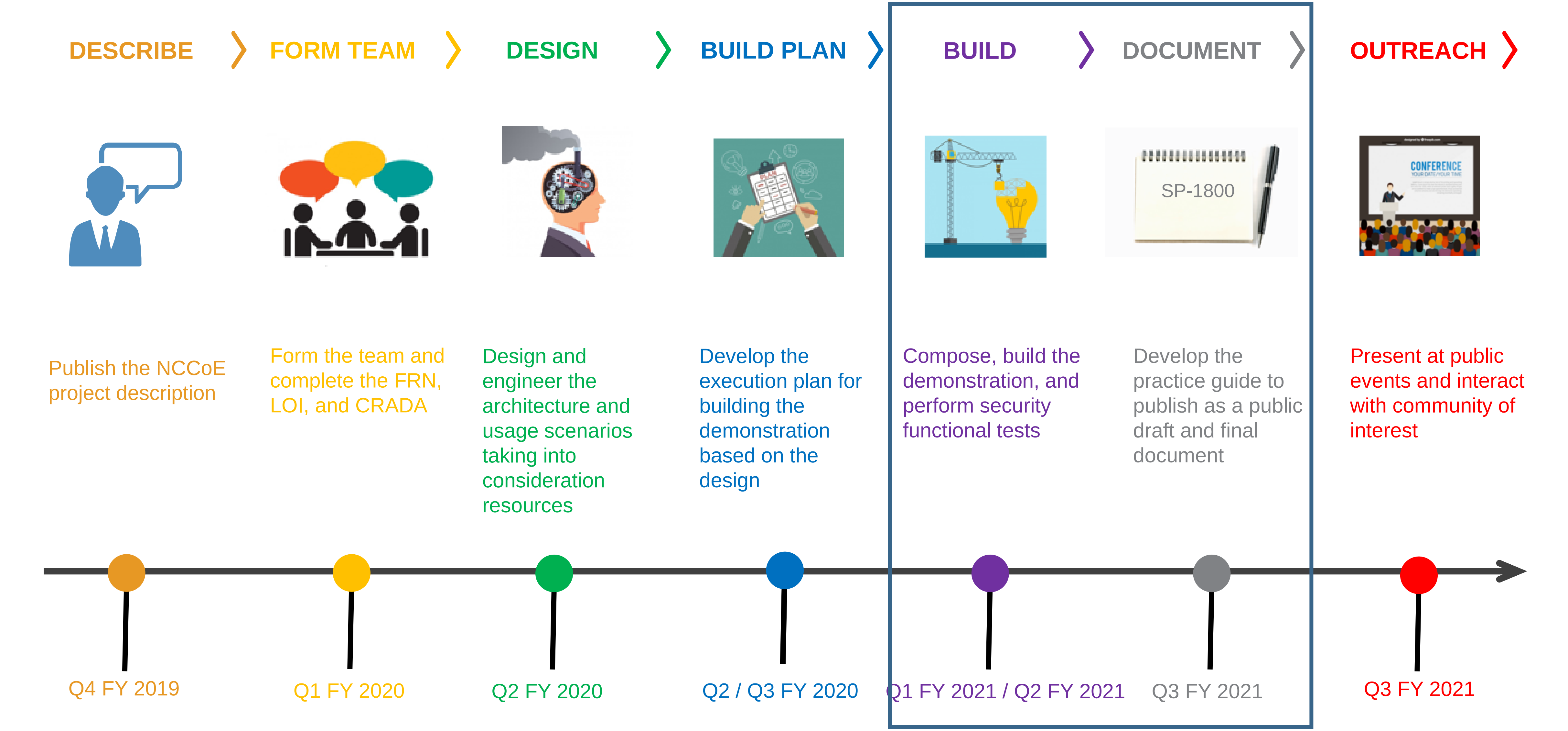
tdi
technologies

tenable

vmware

Project Execution Timeline

SP 180010: Detecting and Protecting Against Data Integrity Attacks in ICS Environments



DESCRIBE

Publish the NCCoE project description

Q4 FY 2019

FORM TEAM

Form the team and complete the FRN, LOI, and CRADA

Q1 FY 2020

DESIGN

Design and engineer the architecture and usage scenarios taking into consideration resources

Q2 FY 2020

BUILD PLAN

Develop the execution plan for building the demonstration based on the design

Q2 / Q3 FY 2020

BUILD

Compose, build the demonstration, and perform security functional tests

Q1 FY 2021 / Q2 FY 2021

DOCUMENT

Develop the practice guide to publish as a public draft and final document

Q3 FY 2021

OUTREACH

Present at public events and interact with community of interest

Q3 FY 2021

Questions?

Contact us:

manufacturing_nccoe@nist.gov